RSA encryption

Coding Challenge Level 3

Greatest common divisor

- The greatest common divisor between two numbers a and b is the largest divisor that a and b have in common.
- Notation

  Divisor 6 = {1,2,3,6}
- Divisor 15 = {1,3,5,15}
- It can be calculated by forming the intersection between the divisors of a and b.
- $A \cap B = \{1,3\}$
- gcd(6,15) = 3

Relatively Prime

- Two numbers a and b are said to be relatively prime (or coprime) if they have no common divisors other than 1. Therefore, the greatest common divisor (gcd) of two relatively prime numbers is 1.
- 15 Teiler = {1,3,4,15} ∩
- 22 Teiler = {1,2,11}
- = {1}
  ggT(15,22) = 1
- Prime Numbers are always relatively prime, as their divisors are only one and themself.

Eulers ϕ-Function

- The Eulers ϕ-function states, how many integers smaller than, are relatively prime to n.

- ϕ(12) = 4
- For large this numbers this is hard to calculate, except if those large numbers are prime. Than the following rule applies:
- ϕ(n) = p-1
- → all numbers smaller than p are relatively prime as it a prime number
- The function is multiplicative:
- ϕ(a*b) = ϕ(a)*ϕ(b)

Key creation

- Chose two big prime numbers (p and q), for maximun secrurity at least 2048 bits better 3072 bits in lenght.
- Calculate N = p*q
- Calculate $\phi(n) = (p-1)*(q-1)$
- Chose e: $1 < e < \varphi(N)$, $ggT(e,\varphi(N)=1$
- Calculate d with: $e*d \equiv 1 \mod \varphi(N)$
- Public key: (N,e)
- Private key: (N,d)

Encryption/Decryption

- Encryption c:
- $c = m^e \bmod N$

Decryption m:

$m = c^d \bmod N$

Solution

- Text translated into Unicode then, encrypted using RSA-encryption:
- N and d for the decryption process can be found in the source code of level2
- Decrypted text: Great job you found the solution [e5crypt10n_1s_k3y.html]

Modulo-Operation

- The modulo-operation a mod b, states the remainder of a division between a and b

12 mod 5 = 2 12 / 5 = 2 remain 2 → 12 = 2 mod 5

18 mod 2 = 0 18 / 2 = 9 remain 0 → 18 = 0 mod 2

3 mod 5 = 3 3 / 5 = 0 remain 3 → 3 = 3 mod 5

N

- 183318841779398497481876434874050693905459924897079723442512456947573840709726951833868036842136600551371224113412470356898439553513860229191941392729483296161138914578533920260224241034889320570621598994695675435130965458705078812452121191800935622571899989070097050342633349962789789632516043783030919419023946325999635361721636817714068353526703235045647792188801812692014941106705404646802721354738167717064321364730979989968448277250181858530421264695221909029106885973683128884208073511184882994512844578898687235099930563454035150577454183982124583953695475378660615152280179603086970792833693321502421922526126353043837673136353316423140419091697780930540877923832019013600392832354129104439589186671343973205730794205032740807092634374958544973719099271967263977193029505747263164865495937060814413523251467227292061582855020814932754502079701976805235106787732509060775466259238314662 39

d

- 1222125611862656649879176232493671292703066165980531489616749712983825604731513012225786912280910670342474827422749802379322930356759068194612942618196555307740926097190226135068161606899262137137477326631304502900873103058033858749680807945339570817145999927133980335617555666418598597550106958553539462793492975506664235744810912118093789023511354900304318614591942770592653248484619749766832262232179913232256558645415878190079717395287775579334400868586695084378131453224813168768223969335309152651301367292901694472992152927227929147960801776614421425132797901886309718614186091023334846314956754643361567790761813233146082052293362037700830286795022600654049080203010575465754518135643476314902910499915681852719644165895457120884951730984949002350480187321544917903427685834464535929313909334232347421675115451190148049120649616345813815751830648392233130055869762026808517307044051310994 7

RSA encrypted message

- [357911, 1481544, 1030301, 912673, 1560896, 32768, 1191016, 1367631, 941192, 32768, 1771561, 1367631, 1601613, 32768, 1061208, 1367631, 1601613, 1331000, 1000000, 32768, 1560896, 1124864, 1030301, 32768, 1520875, 1367631, 1259712, 1601613, 1560896, 1157625, 1367631, 1331000, 32768, 753571, 1030301, 148877, 970299, 1481544, 1771561, 1404928, 1560896, 117649, 110592, 1331000, 857375, 117649, 1520875, 857375, 1225043, 132651, 1771561, 97336, 1124864, 1560896, 1295029, 1259712, 804357]